บทที่ 3

มาตรการทางอาญาสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ

3.1 รูปแบบมาตรการทางอาญาสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

3.1.1 ประหารชีวิต (Capital Punishment)

การลงโทษด้วยวิธีการประหารชีวิตเป็นวิธีการลงโทษที่รุนแรงที่สุด โดยการประหารชีวิตมีจุดมุ่งหมายในการลงโทษ 3 ประการ ได้แก่ ประการแรก เพื่อเป็นการแก้แค้นตอบแทนการกระทำความผิด ประการที่สอง เพื่อให้เกิดความหวาดหวั่นและไม่กล้าที่จะกระทำความผิดและประการสุดท้าย เพื่อเป็นการป้องกันสังคมโดยการตัดผู้กระทำความผิดออกจากสังคมโดยถาวร[1] สำหรับกรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบส่วนใหญ่ไม่ปรากฏว่ามีการนำเอาวิธีการลงโทษในลักษณะนี้มาบังคับ มีแต่เพียงในประเทศสาธารณรัฐประชาชนจีนเท่านั้นที่ปรากฏว่ามีการนำโทษประหารชีวิตมาใช้กับคดีที่เกี่ยวกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

ตัวอย่างเช่น ในปี ค.ศ.2000 ศาลตัดสินลงโทษประหารชีวิตแฮกเกอร์ชาวจีน ในจังหวัด Hang Zhou ประเทศจีน ในข้อหายักยอกเงินในบัญชีลูกค้าจำนวน 1.66 ล้านหยวน หรือประมาณ 200,000 เหรียญสหรัฐ จากธนาคารซึ่งผู้กระทำผิดทำงานอยู่[2]

ข้อสังเกต ในประเทศสาธารณรัฐประชาชนจีน แม้ว่าการลงโทษประหารชีวิตมักจะนำมาใช้กับอาชญากรรมที่ร้ายแรง เช่น ฆาตกรรม ข่มขืนและความผิดต่อทรัพย์สินที่ร้ายแรง เป็นต้น[3] แต่ในปัจจุบันศาลในประเทศสาธารณรัฐประชาชนจีนได้นำเอาโทษประหารชีวิตมาใช้กำหนดโทษ

---

[1] นัทธี จิตสว่าง, หลักทัณฑวิทยา, พิมพ์ครั้งที่ 3(กรุงเทพมหานคร: มูลนิธิพิบูลสงคราม กรมราชทัณฑ์, 2545), น.35.

[2] Russell G. Smith, Peter Grabosky and Gregor Urbas, CYBER CRIMINALS ON TRIAL, (Australia: Ligare Pty Lid, 2004), p.194.

[3] สถาบันกฎหมายอาญา, สารานุกรมกระบวนการยุติธรรมนานาชาติ, แปลจาก Criminal justice profiles of Asia และ Criminal justice systems in Europe and North America, (กรุงเทพมหานคร: สถาบันกฎหมายอาญา, 2540), น.30.

ในกรณีอาชญากรรมทางเศรษฐกิจที่ไม่ร้ายแรงหลายประเภท เช่น การโกงภาษีมูลค่าเพิ่มและการหลบเลี่ยงภาษี การปลอมแปลง ยักยอกและขโมยบัตรเครดิต เป็นต้น ยกตัวอย่างเช่น ในเดือนมีนาคม ค.ศ.1997 ศาลตัดสินลงโทษประหารชีวิต ในคดีขโมยบัตรเครดิต เป็นจำนวนเงิน 62,650 เหรียญสหรัฐ[4]

3.1.2 จำคุก (Imprisonment)

กฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ของต่างประเทศมักจะกำหนดโทษจำคุกเป็นโทษหลักสำหรับความผิดในแต่ละฐานความผิดและศาลในต่างประเทศก็นำโทษจำคุกมาใช้กับคดีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบอย่างกว้างขวางเช่นเดียวกัน ซึ่งกฎหมายของต่างประเทศเกี่ยวกับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่กำหนดโทษจำคุกไว้ในบทบัญญัติดังกล่าว มีตัวอย่างเช่น

ประเทศสหรัฐอเมริกาได้บัญญัติฐานความผิดเกี่ยวกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไว้ใน Computer Fraud and Abuse Act (CFAA) มาตรา 1030(a)(1) – (5) มีรายละเอียดโดยสังเขป ดังนี้

- มาตรา 1030 (a)(1) การเข้าถึงข้อมูลสำคัญโดยมิชอบ เช่น ข้อมูลสำคัญเกี่ยวกับรัฐบาล หรือฝ่ายบริหาร หรือเกี่ยวข้องกับความมั่นคงของประเทศ
- มาตรา 1030 (a)(2) การเข้าถึงข้อมูลเกี่ยวกับสถาบันการเงิน หน่วยงานรัฐ หรือข้อมูลที่สื่อสารระหว่างมลรัฐหรือระหว่างประเทศโดยมิชอบ
- มาตรา 1030 (a)(3) การเข้าถึงคอมพิวเตอร์ของหน่วยงานหรือสำนักงานของรัฐโดยมิชอบ
- มาตรา 1030 (a)(4) การเข้าถึงข้อมูลโดยมิชอบเพื่อเจตนาฉ้อโกง
- มาตรา 1030 (a)(5) การเข้าถึงคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยปราศจากอำนาจ

ทั้งนี้ในมาตรา 1030 (c)(1) – (5) ได้บัญญัติโทษของแต่ละฐานความผิดดังที่กล่าวไว้ข้างต้น โดยมีโทษปรับและโทษจำคุกเป็นโทษหลักของแต่ละฐานความผิด โทษจำคุกสำหรับฐานความผิดเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศสหรัฐอเมริกากำหนดไว้แตกต่างกันไปตาม

[4] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2 , p.223.

ความร้ายแรงแห่งความผิดในแต่ละฐานความผิดและเงื่อนไขในการกระทำความผิดซ้ำ ซึ่งมีอัตราโทษจำคุกขั้นสูงสุดตั้งแต่ 1 – 20 ปีและจำคุกตลอดชีวิต[5]

ยกตัวอย่างคดีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศสหรัฐอเมริกา ซึ่งศาลนำโทษจำคุกมาปรับใช้กับผู้กระทำผิด เช่น

คดี Scott Levine (U.S. v. Levine[6](E.D. Ark) 22 กุมภาพันธ์ 2006) กระทำความผิดในข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ (120 กระทง)และเข้าถึงเครื่องมือในการฉ้อโกง (2 กระทง) ศาลตัดสินลงโทษจำคุก 96 เดือน

คดี Jeanson James Ancheta (U.S. v. Ancheta[7](C.D. Cal.) 8 พฤษภาคม 2006) กระทำความผิดตาม Computer Fraud Abuse Act และ CAN-SPAM Act โดยใช้วิธีการทำให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service: DOS) ทำให้ระบบคอมพิวเตอร์ของหน่วยงานของรัฐเสียหาย รวมทั้งยังเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจเพื่อการฉ้อโกง ศาลตัดสินลงโทษจำคุก 57 เดือนและปรับ 57,000 เหรียญสหรัฐ นอกจากนี้คดีนี้ยังเป็นคดีที่ศาลลงโทษจำคุกสำหรับคดีไวรัสคอมพิวเตอร์นานที่สุดเท่าที่เคยมีมา และศาลยังสั่งริบทรัพย์สินของจำเลย ได้แก่ รถบีเอ็มดับบลิวและอุปกรณ์คอมพิวเตอร์ นอกจากนี้ศาลยังสั่งควบคุมจำเลยหลังปล่อยตัวเป็นระยะเวลา 3 ปี โดยควบคุมการเข้าถึงคอมพิวเตอร์และอินเทอร์เน็ต

คดี Juju Jiang (U.S. v. Jiang[8] (S.D. N.Y.) 28 กุมภาพันธ์ 2005) กระทำความผิดในข้อหาจารกรรมข้อมูลคอมพิวเตอร์ส่วนบุคคล เข้าถึงระบบคอมพิวเตอร์โดยมิชอบและทำลายระบบคอมพิวเตอร์ ศาลตัดสินลงโทษจำคุกเป็นเวลา 27 เดือน ปรับเป็นเงิน 201,620 เหรียญสหรัฐ

---

[5] โปรดดูรายละเอียดเพิ่มเติมใน ผนวก ค.

[6] United States v. Levine, 378 F. Supp. 2d 872 (E.D. Ark., 2005), see also Former Officer of Internet Company Sentenced in Case of Massive Data Theft from Acxiom Corporation,< http://www.usdoj.gov/criminal/cybercrime/levineSent.htm >, 22 February 2006.

[7] "Botherder" Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code, < http://www.usdoj.gov/criminal/cybercrime/anchetaSent.htm >, 8 May 2006.

[8] Queens Man Sentenced to 27 Months' Imprisonment on Federal Charges of Computer Damage, Access Device Fraud and Software Piracy, < http://www.usdoj

คดี Brian A. Salcedo (U.S. v. Salcedo et. al.[9] (W.D. N.C.) 15 ธันวาคม 2004) กระทำความผิดในข้อหาร่วมกันเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจและเอาไปซึ่งข้อมูลบัตรเครดิตเพื่อการฉ้อโกง ศาลตัดสินลงโทษจำคุกเป็นเวลา 108 เดือน ซึ่งในคดีนี้เป็นคดีที่ลงโทษจำคุกอาชญากรคอมพิวเตอร์ที่ยาวนานที่สุด (ซึ่งก่อนหน้านี้มีคดีที่ลงโทษจำคุกยาวนานที่สุด คือ คดี Kevin Mitnick ซึ่งลงโทษจำคุกถึง 68 เดือน)

คดี Jesus Diaz (U.S. v. Diaz[10] (S.D. Fla.) 5 ธันวาคม 2003) กระทำความผิดในข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจและก่อความเสียหายโดยประมาท (Title 18, United States Code, Section 1030(a)(5)(A)(ii)) ถูกศาลตัดสินลงโทษจำคุก 12 เดือนและปรับ 80,713.79 เหรียญสหรัฐ

ส่วนประเทศอังกฤษได้บัญญัติความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไว้ใน Computer Misuse Act 1990 มาตรา 1 โดยผู้กระทำผิดฐานเข้าถึงข้อมูลหรือโปรแกรมคอมพิวเตอร์โดยปราศจากอำนาจ ต้องระวางโทษจำคุกไม่เกิน 6 เดือน ประเทศออสเตรเลียบัญญัติฐานความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไว้ใน The Cybercrime Act 2001 มาตรา 478.1 โดยต้องระวางโทษจำคุกไม่เกิน 2 ปี ประเทศแคนาดา บัญญัติความผิดฐานใช้คอมพิวเตอร์โดยปราศจากอำนาจ (unauthorized use of computer) ในประมวลกฎหมายอาญา มาตรา342.1(1) ต้องระวางโทษจำคุกไม่เกิน 10 ปี นอกจากนี้แล้วยังมีกฎหมายเกี่ยวกับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศอีกหลายประเทศที่กำหนดโทษจำคุกเป็นโทษหลักสำหรับการกระทำผิดในลักษณะดังกล่าว[11]

.gov/criminal/cybercrime/jiangSent.htm >, 28 February 2005.

[9] United States v. Salcedo, 189 Fed. Appx. 197 (4th Cir. 2006), see also Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information, < http://www.usdoj.gov/criminal/cybercrime/salcedo Sent.htm >, 15 December 2004.

[10] Former Hellmann Logistics Computer Programmer Sentenced for Unauthorized Computer Intrusion, < http://www.usdoj.gov/criminal/cybercrime /diazSent.htm >, 5 December 2003.

[11] โปรดดูรายละเอียดใน ผนวก ค.

3.1.3 ปรับหรือชดใช้ความเสียหาย (Fine or Restitution)

สำหรับในคดีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ โทษปรับเป็นรูปแบบโทษที่บัญญัติเป็นโทษหลักและศาลในต่างประเทศนำมาใช้กับผู้กระทำผิดอย่างกว้างขวางเช่นเดียวกับโทษจำคุก ส่วนกรณีการชดใช้ความเสียหายให้แก่เหยื่อในคดีอาญา (criminal restitution) เป็นมาตรการที่ศาลมีคำสั่งให้ผู้กระทำผิดชดใช้ความเสียหายทางการเงิน (financial losses) ที่เกิดขึ้นจากการกระทำความผิดของตนให้แก่เหยื่อ โดยมาตรการดังกล่าวไม่ใช่การลงโทษทางอาญา แต่เป็นมูลหนี้ที่ผู้กระทำผิดมีต่อเหยื่อ[12] บทบัญญัติเกี่ยวกับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศหลายประเทศที่ได้กำหนดโทษปรับเป็นมาตรการลงโทษสำหรับความผิดดังกล่าว ตัวอย่างเช่น ประเทศสหรัฐอเมริกา ได้บัญญัติโทษปรับไว้ในแต่ละฐานความผิดเกี่ยวกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ตาม Computer Fraud and Abuse Act (CFAA) มาตรา 1030 (c)(1) – (5) ซึ่งได้กล่าวไว้แล้วในหัวข้อก่อนหน้านี้ ส่วนกรณีมาตรการชดใช้ความเสียหาย (Restitution) นั้นกฎหมายของประเทศสหรัฐอเมริกามีบัญญัติไว้ใน Title 18, United State Code (U.S.C.), มาตรา 3663A[13] ซึ่งเป็นบทบัญญัติว่าด้วยการชดใช้ความเสียหายในกรณีที่ศาลต้องมีคำสั่งให้ผู้กระทำผิดชดใช้ความเสียหายทางทรัพย์สินให้แก่เหยื่อ[14]

ตัวอย่างคดีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศสหรัฐอเมริกาซึ่งนำโทษปรับและชดใช้ความเสียหายมาปรับใช้กับคดี เช่น

---

[12] Criminal Restitution, <http://www.cted.wa.gov/_CTED/documents/ID_34_Publications.pdf>

[13] Title 18, United State Code (U.S.C.), มาตรา 3663A (b) บัญญัติให้ศาลมีคำสั่งให้ผู้กระทำผิดชดใช้ความเสียหายให้แก่เหยื่อในกรณีต่อไปนี้ (1) ในกรณีการกระทำผิดก่อให้เกิดความเสียหาย สูญเสียหรือทำลายทรัพย์สินของเหยื่อ (2) ในกรณีการกระทำผิดส่งผลให้เกิดอันตรายต่อร่างกายของเหยื่อ (3) ในกรณีการกระทำผิดส่งผลให้เกิดอันตรายต่อชีวิตของเหยื่อ และ (4) กรณีที่เหยื่อต้องสูญเสียรายได้ รวมทั้งค่าใช้จ่ายอันเกี่ยวข้องกับการสืบสวนหรือดำเนินคดีในการกระทำความผิดดังกล่าว

[14] Jennifer S. Granick, “Facking: Calculating Loss in Computer Crime Sentencing,” <http://infosecon.net/workshop/pdf/FakingIt.granick.pdf>

คดี Ehud Tenebaum (U.S. v. Tenebaum[15] (Israel) 18 มีนาคม 1998) กระทำความผิดในข้อหาเข้าถึงระบบคอมพิวเตอร์ของรัฐบาลประเทศสหรัฐอเมริกาและอิสราเอลโดยมิชอบด้วยกฎหมาย ศาลตัดสินลงโทษให้คุมประพฤติเป็นเวลา 12 เดือนและปรับเป็นเงิน 17,000 เหรียญสหรัฐ

คดี Eric Burns (U.S. v. Burns[16] (E.D. VA) 19 พฤศจิกายน 1999) กระทำความผิดในข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจและทำลาย แก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ ศาลตัดสินลงโทษจำคุกเป็นเวลา 15 เดือนและปรับเป็นเงิน 36,240 เหรียญสหรัฐ

คดี Patrick W. Gregory (U.S. v. Gregory[17] (N.D. TX) 6 กันยายน 2000) กระทำความผิดในข้อหาร่วมกันกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจและฉ้อโกงทางโทรคมนาคม (Title 18, United States Code, Sections 371, 1029 (a)(2) and 1030 (a)(5)) ศาลตัดสินจำคุก 26 เดือน ปรับเป็นเงิน 154,529.86 เหรียญสหรัฐ

คดี Kenneth J. Flury (U.S. v. Flury[18] (N.D. Ohio) 18 กุมภาพันธ์ 2006) กระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ ขโมยหมายเลข ข้อมูลบัตรเครดิตและข้อมูลบ่งเฉพาะบุคคลเพื่อการฉ้อโกง ศาลสั่งให้จำเลยชดใช้ค่าเสียหายแก่เหยื่อเป็นจำนวน 300,748.64 เหรียญสหรัฐและชดใช้ให้แก่กองทุนเหยื่ออาชญากรรมเป็นจำนวน 200 เหรียญสหรัฐ

ส่วนประเทศอังกฤษ ได้กำหนดโทษปรับสำหรับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบใน Computer Misuse Act 1990 มาตรา 1 ต้องระวางโทษปรับไม่เกินระดับ 5 ตามตารางมาตรฐาน (ปัจจุบันคือ 5,000 ปอนด์) ประเทศฝรั่งเศส กำหนดโทษปรับสำหรับการกระทำ

---

[15] Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers, <http://www.usdoj.gov/criminal/cybercrime/ ehudpr.htm> , 18 March 1998.

[16] "WEB BANDIT" HACKER SENTENCED TO 15 MONTHS IMPRISONMENT, 3 YEARS OF SUPERVISED RELEASE, FOR HACKING USIA, NATO, WEB SITES, < http://www.usdoj.gov/criminal/cybercrime/burns.htm >, 19 November 1999.

[17] Computer Hacker Sentenced, < http://www.usdoj.gov/criminal/ cybercrime/gregorysen.htm >, 6 September 2000.

[18] Cleveland, Ohio Man Sentenced to Prison for Bank Fraud and Conspiracy, < http://www.usdoj.gov/criminal/cybercrime/flurySent.htm >, 28 February 2006.

ผิดฐานการเข้าถึงระบบประมวลผลข้อมูลโดยอัตโนมัติโดยมิชอบ ในประมวลกฎหมายอาญา มาตรา 323-1 ต้องระวางโทษปรับไม่เกินหนึ่งแสนฟรังค์ ประเทศมาเลเซีย กำหนดโทษปรับในความผิดฐานเข้าถึงโปรแกรมหรือข้อมูลโดยปราศจากอำนาจ ใน COMPUTER CRIMES ACT 1997 มาตรา 3(1)(2) ต้องระวางโทษปรับไม่เกินห้าแสนริงกิต ประเทศสิงคโปร์ กำหนดโทษปรับในความผิดฐานเข้าถึงโปรแกรมหรือข้อมูลใดๆ ในคอมพิวเตอร์โดยปราศจากอำนาจ ตาม Computer misuse Act มาตรา 3-(1) โดยต้องระวางโทษปรับเป็นเงินไม่เกินห้าพันเหรียญ นอกเหนือจากนี้แล้วยังมีอีกหลายประเทศซึ่งกำหนดโทษปรับเป็นโทษหลักสำหรับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ[19]

3.1.4 <u>ริบทรัพย์สิน (Forfeiture)</u>

การริบทรัพย์สินที่ได้ใช้ หรือมีไว้เพื่อใช้ในการกระทำความผิด เป็นโทษที่มีจุดมุ่งหมายเพื่อป้องกันมิให้ผู้กระทำผิดได้มีโอกาสใช้ทรัพย์สินดังกล่าวในการกระทำความผิดนั้นซ้ำอีก สำหรับกรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ทรัพย์สินที่ได้ใช้ หรือมีไว้เพื่อใช้ในการกระทำความผิด ซึ่งศาลมักจะมีคำสั่งให้ริบทรัพย์สิน ได้แก่ อุปกรณ์คอมพิวเตอร์ รวมถึงอุปกรณ์ที่ใช้ในการเชื่อมต่ออินเทอร์เน็ต เช่น โมเด็ม เป็นต้น

ในประเทศสหรัฐอเมริกา การริบทรัพย์สินในคดีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ตาม Computer Fraud and Abuse Act (CFAA) มาตรา 1030(a)(1) – (5) ศาลในสหรัฐอเมริกาอาจมีคำสั่งให้ริบอุปกรณ์หรือเครื่องมือที่ใช้หรือมีส่วนสนับสนุนในการกระทำผิดดังกล่าวได้ ตาม Title 18, United State Code (U.S.C.), มาตรา 982 (a)(2)[20] ทั้งนี้ตัวอย่างคดี

---

[19] โปรดดูรายละเอียดใน ผนวก ค.

[20] Title 18, United State Code (U.S.C.), มาตรา 982 (a)(2) บัญญัติว่า

" ศาล, ในกรณีที่พิพากษาลงโทษผู้ใดในความผิดตามบทบัญญัติดังต่อไปนี้

(A) .....

(B) มาตรา 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487, 488, 501, 502, 510, 542, 545, 842, 844, 1028, 1029, หรือ 1030

จะต้องมีคำสั่งให้ริบทรัพย์สินซึ่งเกิดขึ้น หรือได้รับมาจาก หรือใช้ในการกระทำผิดดังกล่าวข้างต้น ไม่ว่าโดยตรงหรือโดยอ้อมให้ตกเป็นของสหรัฐอเมริกา..."

เกี่ยวกับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศสหรัฐอเมริกา ซึ่งศาลได้นำเอามาตรการริบทรัพย์สินอันได้แก่ อุปกรณ์คอมพิวเตอร์ของผู้กระทำผิดมาใช้ มีตัวอย่างเช่น

คดี Jeanson James Ancheta (United States v. Ancheta[21]) ซึ่งกระทำความผิดตาม Computer Fraud Abuse Act และ CAN-SPAM Act โดยใช้วิธีการทำให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service: DOS) ทำให้ระบบคอมพิวเตอร์ของหน่วยงานของรัฐเสียหาย รวมทั้งยังเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจเพื่อการฉ้อโกง โดยศาลในคดีนี้มีคำสั่งให้ริบทรัพย์สินของจำเลย อันได้แก่ รถบีเอ็มดับบลิวและอุปกรณ์คอมพิวเตอร์ที่ใช้ในการกระทำความผิด

วันที่ 10 มีนาคม ค.ศ.1997 ศาลมีคำสั่งริบอุปกรณ์คอมพิวเตอร์ทั้งหมดที่ใช้ในการกระทำความผิดโดยผู้กระทำผิดซึ่งเป็นเยาวชนเจาะระบบคอมพิวเตอร์ของท่าอากาศยาน Worcester ในเมือง Rutland มลรัฐ Massachusetts ประเทศสหรัฐอเมริกา ส่งผลให้เกิดความเสียหายต่อระบบบริการโทรศัพท์ในพื้นที่ของเมือง Rutland และนอกจากนี้ผู้กระทำผิดยังเจาะระบบคอมพิวเตอร์ของร้านขายยา รวมทั้งยังได้ดาวน์โหลดข้อมูลส่วนบุคคลเกี่ยวกับใบสั่งจ่ายยาของลูกค้าไปด้วย นอกจากศาลจะลงโทษริบอุปกรณ์คอมพิวเตอร์ของผู้กระทำผิดรายนี้แล้วยังมีคำสั่งคุมประพฤติผู้กระทำผิดเป็นระยะเวลา 2 ปี และในระหว่างการคุมประพฤติห้ามผู้กระทำผิดครอบครองโมเด็มรวมทั้งยังต้องชดใช้ความเสียหายให้แก่บริษัทโทรศัพท์และทำงานบริการสังคมเป็นเวลา 250 ชั่วโมง[22]

3.1.5 <u>การจำกัดการเข้าถึงระบบคอมพิวเตอร์ (Restricted Access to Computers)</u>

ในคดีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบนั้น ในระหว่างการคุมประพฤติหรือการควบคุมสอดส่องหลังการปล่อยตัว (Supervised Release) ศาลในต่างประเทศมีการ

---

[21] United States v. Ancheta, Case Number: CR05-106 , The Central District of California, United States District Court, (February 2005), available at <http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>; see also "Botherder" Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code, < http://www.usdoj.gov/criminal/cybercrime/anchetaSent.htm >,8 May 2006.

[22] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2 ,p.179.

กำหนดเงื่อนไขในการควบคุมความพฤติกรรมของผู้กระทำผิดมิให้เข้าไปเกี่ยวข้องหรือใช้งานคอมพิวเตอร์และอินเทอร์เน็ต ทั้งนี้โดยมีวัตถุประสงค์หลักสองประการ คือ ประการแรกเพื่อป้องกันการกระทำความผิดซ้ำของผู้กระทำผิด และประการที่สองเพื่อป้องกันความปลอดภัยให้แก่สังคม เงื่อนไขในลักษณะเช่นนี้ถูกนำมาใช้สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างกว้างขวางไม่จำกัดแต่เฉพาะกรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบเท่านั้น แต่ยังรวมไปถึงกรณีการกระทำความผิดโดยการดาวน์โหลดภาพลามกอนาจารของเด็ก (Child-pornography) จากอินเทอร์เน็ตด้วย[23]

ในประเทศสหรัฐอเมริกา การกำหนดเงื่อนไขเพื่อคุมความประพฤติ (Conditions of Probation) และการกำหนดเงื่อนไขควบคุมสอดส่องหลังการปล่อยตัว (Conditions of Supervised Release) มีบัญญัติไว้ใน Title 18, United State Code (U.S.C.), มาตรา 3553 มาตรา 3563 และมาตรา 3583 โดยในมาตรา 3553 (a) ได้บัญญัติรายละเอียดเกี่ยวกับปัจจัยสำคัญที่ศาลพึงพิจารณาในการพิพากษาลงโทษ ซึ่งศาลจะต้องคำนึงถึง

(1) สภาพและพฤติการณ์ของความผิด รวมถึงภูมิหลังและสภาพตัวผู้กระทำผิด (the nature and circumstances of the offense and the history and characteristics of the defendant)

(2) ความจำเป็นในการวางมาตรการลงโทษ กล่าวคือ

(A) เพื่อตอบสนองความร้ายแรงของความผิด สนับสนุนการเคารพต่อกฎหมาย และเพื่อให้มีการลงโทษที่มีความยุติธรรม (just punishment)

(B) เพื่อข่มขู่ยับยั้งพฤติกรรมการกระทำผิด

(C) ป้องกันสังคมจากการกระทำความผิดซ้ำของผู้กระทำผิด และ

(D) เพื่อจัดให้ผู้กระทำผิดได้รับการศึกษา อบรมทางวิชาชีพ การรักษาพยาบาล และการปฏิบัติต่อผู้กระทำผิดให้มีประสิทธิภาพสูงสุด

ส่วนในบทบัญญัติ Title 18, United State Code (U.S.C.), มาตรา 3563 เป็นบทบัญญัติเกี่ยวกับการกำหนดเงื่อนไขเพื่อคุมความประพฤติ และในมาตรา 3583 เป็นบทบัญญัติเกี่ยวกับการกำหนดเงื่อนไขเพื่อควบคุมสอดส่องหลังการปล่อยตัว โดยในมาตรา 3563 (b) บัญญัติให้อำนาจศาลในการใช้ดุลพินิจกำหนดเงื่อนไขเพื่อคุมความประพฤติ (Discretionary Conditions) โดยคำนึงถึงปัจจัยสำคัญที่ศาลพึงพิจารณาในการพิพากษาลงโทษตามที่กำหนดไว้

---

[23] *Ibid*, pp.119-121.

ในมาตรา 3553 (a)(1) และ (2) ทั้งนี้การกำหนดเงื่อนไขซึ่งเป็นการจำกัดตัดสิทธิเสรีภาพและทรัพย์สินของผู้กระทำผิดจะต้องกระทำเท่าที่จำเป็นอย่างสมเหตุสมผลเพื่อวัตถุประสงค์ตามบทบัญญัติ มาตรา 3553 (a)(2) เท่านั้น ส่วนกรณีบทบัญญัติในมาตรา 3583 ได้บัญญัติในลักษณะเดียวกันกับมาตรา 3563 โดยการกำหนดเงื่อนไขเพื่อควบคุมสอดส่องหลังการปล่อยตัว ศาลจะต้องพิจารณาจากปัจจัยตามที่กำหนดไว้ในมาตรา 3553 (a)(1) และ (2) เป็นหลักเกณฑ์สำคัญ

เงื่อนไขในการเข้าถึงระบบคอมพิวเตอร์ซึ่งกำหนดโดยศาล ก่อให้เกิดการวิพากษ์วิจารณ์ในแง่ของการเข้มงวดในการลงโทษมากเกินขอบเขตหรือไม่ อีกทั้งอาจเข้าข่ายเป็นการปิดกั้นสิทธิของผู้ต้องโทษมากเกินไปหรือไม่ คดีที่ได้รับความสนใจเกี่ยวกับเรื่องนี้เป็นอย่างยิ่ง คือ คดีของนายเควิน มิตนิก[24] ศาลกำหนดโทษจำคุกเป็นเวลา 5 ปี และมีคำสั่งให้ชดใช้ค่าเสียหายให้แก่เหยื่อเป็นเงิน 4,125 เหรียญสหรัฐ และต้องมอบเงินที่จะได้มาจากการขายเรื่องราวเกี่ยวกับการกระทำความผิดของเขาให้แก่เหยื่อด้วย นอกจากนี้ศาลยังกำหนดเงื่อนไขในระหว่างพักการลงโทษเป็นระยะเวลา 3 ปี ซึ่งในประเด็นนี้ที่ทำให้เกิดเสียงวิพากษ์วิจารณ์ในเวลาต่อมาว่าเป็นการกำหนดมาตรการที่เข้มงวดเกินไปหรือไม่ โดยรายละเอียดของเงื่อนไขที่ศาลกำหนดมีดังต่อไปนี้

"...ห้ามกระทำการใด ๆ ดังต่อไปนี้ โดยปราศจากความเห็นชอบเป็นลายลักษณ์อักษรของพนักงานคุมประพฤติ

1. ครอบครองหรือใช้ไม่ว่าด้วยวัตถุประสงค์ใด ดังต่อไปนี้
   1.1 อุปกรณ์คอมพิวเตอร์
   1.2 ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์
   1.3 โมเด็ม
   1.4 อุปกรณ์ใด ๆ สำหรับต่อพ่วงหรือสนับสนุนสำหรับคอมพิวเตอร์
   1.5 เครื่องคอมพิวเตอร์แบบพกพา อุปกรณ์จัดการข้อมูลส่วนตัว (PDA – Personal Digital Assistant) หรือโทรศัพท์มือถือ
   1.6 โทรศัพท์แบบเซลลูล่า (Cellular telephone) หรือโทรศัพท์มือถือ

---

[24] United States v. Mitnick, 145 F. 3d 1342 (9th Cir. 1998); see also Christopher M.E. Painter, "Supervised Release and Probation Restrictions in Hacker Cases," <http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm>

1.7 โทรทัศน์หรือเครื่องมือสำหรับอุปกรณ์สื่อสารออนไลน์ อินเทอร์เน็ต หรือการเข้าถึงเครือข่ายคอมพิวเตอร์อื่น

1.8 อุปกรณ์ทางอิเล็กทรอนิกส์อื่นใด ซึ่ง ณ ปัจจุบันหรือด้วยเทคโนโลยีที่จะมีในอนาคตสามารถทำให้เป็นเสมือนระบบคอมพิวเตอร์ได้ หรือสามารถทำให้เข้าถึงระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์หรือเครือข่ายโทรคมนาคม (telecommunications network) ยกเว้นกรณีการครอบครองโทรศัพท์ชนิดใช้สาย (land line) ตามปกติ

2. ทำงานหรือให้บริการสำหรับบุคคลใด ๆ ซึ่งมีความเกี่ยวข้องกับธุรกิจด้านคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์หรือโทรคมนาคม และต้องอยู่ในสภาวะที่ทำให้สามารถเข้าถึงคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องกับคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์

3. เข้าถึงคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์หรือการติดต่อสื่อสารแบบไร้สาย (wireless communication) ในรูปแบบอื่นด้วยตนเองหรือโดยผ่านบุคคลที่สาม

4. ทำหน้าที่ในฐานะที่ปรึกษา (consultant or advisor) ของบุคคลหรือกลุ่มบุคคลซึ่งมีความเกี่ยวข้องกิจการด้านคอมพิวเตอร์

5. ได้มาหรือครอบครองรหัสคอมพิวเตอร์ (computer code) ใด ๆ (รวมถึงรหัสลับ (computer password) ด้วย) รหัสเข้าถึงโทรศัพท์ชนิดเซลลูล่า หรืออุปกรณ์ในการเข้าถึงอื่นใดที่สามารถทำให้ผู้กระทำความผิดใช้ ได้มา แลกเปลี่ยน หรือเปลี่ยนแปลงข้อมูลในระบบฐานข้อมูลของคอมพิวเตอร์หรือโทรคมนาคม

6. ใช้หรือครอบครองอุปกรณ์ โปรแกรมหรือเทคนิคในการเข้ารหัสข้อมูลสำหรับคอมพิวเตอร์

7. เปลี่ยนแปลง หรือครอบครองอุปกรณ์โทรศัพท์ โทรศัพท์ดัดแปลง หรืออุปกรณ์โทรคมนาคมอื่นใด

8. ใช้นามแฝง หรือแสดงตัวตนอันเป็นเท็จ (ผู้กระทำผิดจะต้องใช้ชื่อจริงเท่านั้น)”

แต่อย่างไรก็ตาม ฝ่ายทนายของเควิน มิตนิกได้อุทธรณ์คำสั่งของศาลดังกล่าว โดยได้คัดค้านว่า คำสั่งดังกล่าวฝ่าฝืนบทแก้ไขเพิ่มเติมรัฐธรรมนูญ ฉบับที่ 1 (first amendment) เนื่องจากเป็นคำสั่งที่ไม่ชัดแจ้ง คลุมเครือและเป็นการจำกัดสิทธิของจำเลยมากเกินควร ต่อมาศาล

อุทธรณ์ได้พิจารณาและตัดสินว่า เงื่อนไขดังกล่าวมีเหตุมีผลรับฟังได้ เนื่องจากเป็นการออกคำสั่งเพื่อป้องกันพฤติกรรมอาชญากรของผู้กระทำผิดและยังเป็นการป้องกันสังคมส่วนรวมอีกด้วย[25]

นอกจากคดีของเควิน มิตนิกที่ศาลนำเอารูปแบบของเงื่อนไขในการควบคุมพฤติกรรมของผู้กระทำผิดในการเข้าถึงคอมพิวเตอร์และอินเทอร์เน็ต ศาลในต่างประเทศยังนำมาตรการบังคับในลักษณะเช่นนี้ไปใช้ในคดีอื่น ๆ อีกหลายคดี ยกตัวอย่างเช่น

คดี Jerome T. Heckenkamp (U.S. v. Heckenkamp[26] (N.D. Cal.) 25 เมษายน 2005) กระทำความผิดในข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจและทำลายระบบคอมพิวเตอร์ ศาลลงโทษจำคุก 8 เดือนและกักขังที่บ้านและควบคุมด้วยเครื่องอิเล็กทรอนิกส์เป็นเวลา 8 เดือนโดยห้ามจำเลยใช้งานคอมพิวเตอร์เพื่อเข้าถึงระบบอินเทอร์เน็ตโดยไม่ได้รับความยินยอมจากพนักงานคุมประพฤติ

คดี Jeanson James Ancheta (United States v. Ancheta[27]) ซึ่งกระทำความผิดตาม Computer Fraud Abuse Act และ CAN-SPAM Act โดยใช้วิธีการทำให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service: DOS) ทำให้ระบบคอมพิวเตอร์ของหน่วยงานของรัฐเสียหาย รวมทั้งยังเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจเพื่อการฉ้อโกง ศาลในคดีนี้มีคำสั่งให้ควบคุมสอดส่องจำเลยหลังการปล่อยตัวเป็นระยะเวลา 3 ปี โดยให้ควบคุมการเข้าถึง

---

[25] United States v. Mitnick, 145 F. 3d 1342 (9th Cir. 1998); and see also Christopher M.E. Painter, “Supervised Release and Probation Restrictions in Hacker Cases,” <http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm>

[26] United States v. Heckenkamp, 482 F.3d 1142 (9th Cir.2007), see also Former Computer Science Graduate Student Sentenced for Hacking Major Corporations: Defendant Jerome Heckenkamp Defaced Web Pages and Installed "Sniffer" Programs to Steal Passwords , < http://www.usdoj.gov/criminal/ cybercrime /heckenkampSent.htm >, 25 April 2005.

[27] United States v. Ancheta, Case Number: CR05-106 , The Central District of California, United States District Court, (February 2005), available at <http://fl1.findlaw .com/news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>; see also "Botherder" Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code, < http://www.usdoj.gov/criminal/cybercrime/anchetaSent.htm >,8 May 2006.

คอมพิวเตอร์และอินเทอร์เน็ต

3.1.6 การควบคุมสอดส่องการใช้คอมพิวเตอร์ (Monitoring Computer Usage)

การควบคุมสอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตของผู้กระทำความผิดเป็นเงื่อนไขเพื่อคุมความประพฤติอีกรูปแบบหนึ่งที่ศาลนำมาใช้สำหรับคดีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ทั้งนี้เนื่องจากในบางกรณีเงื่อนไขการห้ามเข้าถึงหรือใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ตในระหว่างการคุมประพฤติหรือการพักการลงโทษไม่อาจนำมาใช้กับบางคดีได้ จึงจำเป็นที่จะต้องมีการควบคุมสอดส่องพฤติกรรมของผู้ถูกคุมความประพฤติหรือพักการลงโทษเกี่ยวกับการใช้งานคอมพิวเตอร์หรืออินเทอร์เน็ตว่ามีแนวโน้มการกระทำความผิดซ้ำหรือมีการละเมิดเงื่อนไขของคำสั่งศาลในเรื่องอื่น ๆ หรือไม่ เช่น กลับไปติดต่อกับกลุ่มแฮกเกอร์หรือเข้าไปในเว็บไซต์เกี่ยวกับแฮกเกอร์ซึ่งศาลมีคำสั่งห้ามไว้ เป็นต้น

ปัจจุบันหน่วยงานคุมประพฤติในประเทศสหรัฐอเมริกาได้นำเอาเทคโนโลยีในการควบคุมสอดส่องการใช้คอมพิวเตอร์ของผู้กระทำผิดมาใช้กันอย่างกว้างขวาง[28] SEARCH หรือสมาคมข้อมูลและสถิติกระบวนการยุติธรรมแห่งชาติ (the National Consortium for Justice Information and Statistics)[29] ได้รวบรวมข้อมูลเกี่ยวกับโปรแกรมในเชิงพาณิชย์ซึ่งพนักงานคุมประพฤติและพนักงานสืบเสาะ (pretrial services officers) ในประเทศสหรัฐอเมริกานิยมนำมาใช้ในการควบคุมสอดส่องการใช้คอมพิวเตอร์ของผู้กระทำผิด มีดังต่อไปนี้[30]

- Boss Everywhere (http://www.bosseveryware.com)
- Desktop Surveillance (http://www.omniquaid.com)
- Eblaster (http://www.eblaster.com)
- PC Activity Monitor Pro (http://www.pcacme.com)
- STAR-Rtm PC and Internet Monitor Pro (http://www.iopus.com)

---

[28] Mark Sherman, “Special Needs Offenders : Cyber Crime and Cyber Terrorism,” <http://www.fjc.gov/public/pdf.nsf/lookup/SNOCyb02.pdf/$file/SNOCyb02.pdf>, April 2002.

[29] http://www.search.org

[30] Mark Sherman, *Supra note* 24, p.7.

โปรแกรมดังกล่าวเป็นโปรแกรมในเชิงพาณิชย์ซึ่งจำเป็นต้องใช้ต้นทุนในการจัดซื้อเป็นจำนวนมาก ราคาของโปรแกรมในด้านการควบคุมสอดส่องจำหน่ายชุดละ 50 -175 เหรียญสหรัฐฯ ส่วนโปรแกรมด้านนิติวิทยาศาสตร์มีราคาถึงชุดละ 500 -1,700 เหรียญสหรัฐฯ[31] ในด้านของคุณสมบัติการใช้งานของแต่ละโปรแกรมจะมีรูปแบบการทำงานที่แตกต่างกันออกไป แต่อย่างไรก็ตามคุณสมบัติพื้นฐานที่จะตอบสนองการใช้งานในด้านการควบคุมสอดส่องการใช้คอมพิวเตอร์ของผู้ถูกคุมความประพฤติได้ จะต้องมีคุณสมบัติดังต่อไปนี้

- บันทึกการใช้งานคอมพิวเตอร์ของผู้ใช้ โดยวิธีการจับภาพหน้าจอ (screen capturing) หรือ จับข้อมูลการกดแป้นพิมพ์ (keystroke capturing)
- บันทึกข้อมูลการใช้งานอินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์และการสนทนาออนไลน์ รวมถึงกลั่นกรองข้อมูลหรือเว็บไซต์ต้องห้ามได้
- ตรวจสอบการติดตั้งโปรแกรมต้องห้ามได้ (Identify the case of unauthorized software installation)
- ตรวจสอบการใช้งานจากคำค้น (keyword or phrase detected)

เทคโนโลยีในการควบคุมสอดส่องการใช้คอมพิวเตอร์ระหว่างการคุมประพฤติหรือพักการลงโทษในปัจจุบันสามารถจำแนกได้เป็น 3 รูปแบบ ดังต่อไปนี้[32]

(ก) โปรแกรมทางนิติวิทยาศาสตร์ (Forensic Software)

เป็นโปรแกรมที่เจ้าหน้าที่นำมาใช้ในการจำลองข้อมูลทั้งหมดในคอมพิวเตอร์ของผู้กระทำผิด ซึ่งเปรียบเสมือนการถอดแบบหน่วยความจำทั้งหมดจากฮาร์ดดิสก์ในคอมพิวเตอร์ของผู้กระทำผิด ทำให้เจ้าหน้าที่สามารถนำข้อมูลดังกล่าวไปตรวจสอบทางนิติวิทยาศาสตร์ได้ต่อไป ตัวอย่างโปรแกรมทางนิติวิทยาศาสตร์ที่ใช้ในปัจจุบันนี้ เช่น EnCase (http://www.encase.com) และ Ilook investigator (http://www.ilook-forensics.org) เป็นต้น

---

[31] *Ibid.*

[32] Shauna Curphey, “United States v. Liftshitz, warrantless computer monitoring and the fourth amendment,” <http://lls.lls.edu/documents/documents/curphey.pdf>

ซึ่งข้อดีของการจำลองข้อมูลดังกล่าว คือ สามารถตรวจสอบข้อมูลในคอมพิวเตอร์ของผู้กระทำผิดได้อย่างละเอียด แม้กระทั่งข้อมูลที่ถูกซ่อนหรือลบไปแล้วก็สามารถตรวจสอบได้ แต่วิธีการดังกล่าวมีข้อเสีย คือ ต้องใช้เวลามากในการจำลองข้อมูล ฉะนั้นจึงจำเป็นที่จะต้องยึดคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องของผู้กระทำผิดไปเพื่อตรวจในห้องปฏิบัติการ และด้วยวิธีการตรวจสอบข้อมูลคอมพิวเตอร์ส่วนตัวของผู้กระทำผิดอย่างละเอียดจึงเป็นก้าวล่วงสิทธิส่วนบุคคลของผู้กระทำผิดอย่างมิอาจหลีกเลี่ยงได้ รวมทั้งอาจมีปัญหาในทางปฏิบัติหากคอมพิวเตอร์ดังกล่าวเป็นคอมพิวเตอร์ประจำบ้านที่อนุญาตให้สมาชิกคนอื่น ๆ สามารถใช้งานได้ด้วย[33]

ส่วนโปรแกรมรูปแบบอื่นซึ่งทำงานโดยการเล่นแผ่นซีดีโปรแกรมจากเครื่องคอมพิวเตอร์ของผู้ถูกคุมความประพฤติและสามารถเลือกข้อมูลเป้าหมายโดยการใช้คำค้น (keyword) ซึ่งกำหนดขึ้นโดยพนักงานคุมประพฤติ ยกตัวอย่างเช่น โปรแกรม ComputerCop Professional P3 และ ComputerCop Forensic (http://www.computercop.com) แม้ว่ารูปแบบดังกล่าวจะเป็นการก้าวล่วงสิทธิส่วนบุคคลของผู้ถูกคุมความประพฤติน้อยกว่ารูปแบบแรก แต่อย่างไรก็ตามวิธีการนี้ยังต้องอาศัยพนักงานคุมประพฤติในการเข้าไปปฏิบัติงานที่บ้านของผู้ถูกคุมความประพฤติโดยตรง[34]

(ข) โปรแกรมควบคุมสอดส่อง (Monitoring Software)

เป็นโปรแกรมที่ทำงานในเครื่องคอมพิวเตอร์ของผู้ถูกคุมความประพฤติและรวบรวมข้อมูลสำคัญที่เกี่ยวกับการใช้งานต่าง ๆ ของผู้ถูกคุมความประพฤติไว้ เช่น การเรียกใช้โปรแกรม การใช้งานอินเทอร์เน็ต การพูดคุยออนไลน์ หรือการติดต่อสื่อสารผ่านทางจดหมายอิเล็กทรอนิกส์ (email) เป็นต้น โดยข้อมูลที่รวบรวมไว้ดังกล่าวอาจถูกส่งไปยังพนักงานคุมประพฤติผ่านทางจดหมายอิเล็กทรอนิกส์ หรืออาจถูกเก็บเอาไว้ในเครื่องคอมพิวเตอร์ของผู้ถูกคุมความประพฤติเพื่อให้พนักงานคุมประพฤติสามารถตรวจสอบได้ในภายหลัง ด้วยรูปแบบการรายงานผลไปยังพนักงานคุมประพฤติโดยตรงผ่านทางจดหมายอิเล็กทรอนิกส์ โดยพนักงานคุมประพฤติไม่จำต้องไปปฏิบัติงานที่บ้านของผู้ถูกคุมความประพฤติโดยตรง จึงเป็นรูปแบบที่ก้าวล่วงสิทธิส่วนบุคคลของผู้ถูก คุมความประพฤติน้อยกว่ารูปแบบอื่น

---

[33] United States v. Lifshitz, 369 F.3d 173, 193 (2d Cir. 2004).

[34] Shauna Curphey, *Supra Note* 28 .

(ค) โปรแกรมกลั่นกรองการใช้อินเทอร์เน็ต (Filtering or Blocking Software)

เป็นโปรแกรมที่จำกัดการเข้าถึงเว็บไซต์ต้องห้าม โดยโปรแกรมดังกล่าวจะสามารถทำงานได้ทั้งในระดับเครือข่ายคอมพิวเตอร์ภายในของผู้ถูกคุมความประพฤติ หรือในระดับของผู้ให้บริการอินเทอร์เน็ต (ISP: Internet Service Provider) หรือในเครื่องแม่ข่ายภายนอกซึ่งสำรองข้อมูลเว็บไซต์เอาไว้ (off-site server)[35] ข้อดีของการใช้โปรแกรมในลักษณะนี้ คือ เข้าไปก้าวล่วงสิทธิส่วนบุคคลของผู้ถูกคุมความประพฤติน้อยกว่ารูปแบบอื่นเนื่องจากเป็นแต่เพียงการปิดกั้นการเข้าถึงเฉพาะเว็บไซต์ที่ต้องห้ามเท่านั้น ทั้งนี้โดยไม่ได้เข้าไปตรวจสอบการใช้งานส่วนตัวของผู้ถูกคุมความประพฤติแต่อย่างใด[36]

แต่อย่างไรก็ตามมาตรการนี้มีข้อเสีย คือ ประการแรก โปรแกรมในลักษณะดังกล่าวบางโปรแกรมอาจมีประสิทธิภาพในการทำงานน้อยมาก กล่าวคือ ผู้ถูกคุมความประพฤติซึ่งมีความรู้ในทางเทคนิคคอมพิวเตอร์อาจใช้วิธีการในการหลบเลี่ยงหรือใช้เทคนิคต่าง ๆ ในการฝ่าฝืนข้อห้ามนี้ได้โดยง่าย ประการต่อมา เป็นเรื่องยากที่จะสามารถระบุเว็บไซต์ต้องห้ามได้ครอบคลุมทั้งหมด เนื่องจากโลกในอินเทอร์เน็ตเติบโตและพัฒนาอย่างรวดเร็ว มีเว็บไซต์ใหม่ ๆ เกิดขึ้นอยู่ตลอดเวลา จึงเป็นไปไม่ได้อย่างยิ่งที่พนักงานคุมประพฤติจะสามารถใช้วิธีการดังกล่าวในการปิดกั้นการเข้าถึงเว็บไซต์ที่มีลักษณะเข้าข่ายต้องห้ามได้อย่างสมบูรณ์แบบ ประการสุดท้าย การทำงานของโปรแกรมดังกล่าวทำงานแต่เฉพาะการปิดกั้นการเข้าถึงเว็บไซต์ต้องห้ามเท่านั้น แต่ไม่อาจปิดกั้นการรับหรือส่งออกไปซึ่งข้อมูลที่ต้องห้ามผ่านทางจดหมายอิเล็กทรอนิกส์[37]

ยกตัวอย่างคดีที่ศาลมีคำสั่งควบคุมสอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตของผู้กระทำความผิด เช่น ในคดีแรกผู้กระทำผิดโจมตีระบบคอมพิวเตอร์โดยวิธีการปฏิเสธการให้บริการ หรือ Denial of Service ศาลตัดสินลงโทษจำคุก 3 เดือน และให้กักขังที่บ้าน (Home Confinement) เป็นเวลา 3 เดือน นอกจากนี้ยังต้องทำงานบริการสังคมเป็นเวลา 240 ชั่วโมง หลังจากถูกปล่อยตัวจะต้องอยู่ในความควบคุมสอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตโดยพนักงานคุมประพฤติเป็นระยะเวลา 1 ปี[38]

---

[35] *Ibid.*

[36] *Ibid.*

[37] *Ibid.*

[38] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2, p.121.

คดีที่สอง เป็นคดีที่ผู้กระทำผิดซึ่งเป็นอดีตลูกจ้างของบริษัทผู้เสียหายได้โจมตีระบบคอมพิวเตอร์ของบริษัทผู้เสียหาย ศาลตัดสินลงโทษจำคุกเป็นเวลา 16 เดือนและผู้กระทำความผิดจะต้องยินยอมให้เจ้าหน้าที่ตรวจค้นสอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์ของเขาได้โดยไม่จำต้องบอกกล่าวล่วงหน้า นอกจากนี้เขาจะต้องแจ้งพฤติกรรมการกระทำความผิดของเขาให้นายจ้างคนใหม่ในอนาคตได้รับทราบและจะต้องเข้ารับการบำบัดทางจิตด้วย[39]

3.1.7 <u>การกักขังที่บ้านและการควบคุมโดยเครื่องมืออิเล็กทรอนิกส์ (Home Confinement and Electronic Monitoring)</u>

บางกรณีศาลอาจจะมีคำสั่งให้กักขังผู้กระทำความผิดในที่อยู่อาศัยของตน หรือมีการควบคุมผู้กระทำความผิดโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ในระหว่างการคุมประพฤติหรือพักการลงโทษ โดยการกักขังที่บ้าน (home confinement or house arrest or home detention) เป็นการกำหนดให้ผู้กระทำผิดอยู่ในบ้านของตนเองทุกวันในช่วงเวลาหนึ่งจะออกนอกบ้านได้เฉพาะกรณีไปทำงาน ไปเรียนหรือไปรับคำปรึกษา แนะนำ โดยวิธีการกักขังที่บ้านนี้อาจตรวจสอบผ่านทางโทรศัพท์และการออกไปสอดส่องที่บ้าน หรืออาจผ่านทางเครื่องมืออิเล็กทรอนิกส์ ที่มักจะเรียกว่า “การควบคุมด้วยเครื่องอิเล็กทรอนิกส์ (Electronic Monitoring – EM หรือ Electronic Surveillance)”[40]

ในประเทศสหรัฐอเมริกา มาตรการกักขังที่บ้านและการควบคุมด้วยเครื่องมืออิเล็กทรอนิกส์เป็นเงื่อนไขเพื่อคุมความประพฤติอีกประเภทหนึ่ง เช่นเดียวกันกับเงื่อนไขในการคุมความประพฤติกรณีอื่น ๆ ซึ่งได้กล่าวไปแล้วข้างต้น โดยมาตรการนี้ศาลในประเทศสหรัฐอเมริกาจะนำมาใช้กับผู้กระทำผิดในระหว่างการคุมประพฤติ การพักการลงโทษ การควบคุมสอดส่องหลัง

---

[39] *Ibid*, p.121.

[40] ศักดิ์ชัย เลิศพานิชพันธุ์, “การปฏิบัติต่อผู้กระทำผิดในชุมชนกับการใช้มาตรการลงโทษระดับกลาง,” ใน <u>กระบวนทัศน์ใหม่ของกระบวนการยุติธรรมในการปฏิบัติต่อผู้กระทำผิด</u> การประชุมทางวิชาการระดับชาติว่าด้วยงานยุติธรรม ครั้งที่ 1 (กรุงเทพมหานคร: โรงพิมพ์คุรุสภา, 2547), น.265-266.

การปล่อยตัวหรือในระหว่างการปล่อยตัวก่อนการพิจารณา (pretrial release) ทั้งนี้มาตรการกักขังที่บ้านในประเทศสหรัฐอเมริกาจะแบ่งออกเป็น 3 ระดับ[41] คือ

- Curfew เป็นการกำหนดให้อยู่ที่บ้านทุกวันในช่วงเวลาที่กำหนดแน่นอน
- Home Detention เป็นการกำหนดให้อยู่ในบ้านตลอดเวลา เว้นแต่จะได้รับอนุญาตล่วงหน้า และในช่วงเวลาที่กำหนดไว้ เช่น เวลาไปทำงาน โรงเรียน บำบัด โบสถ์ เวลานัดของพนักงานอัยการหรือศาล หรือในเวลาอื่นใด ๆ ซึ่งศาลมีคำสั่ง
- Home incarceration เป็นการกักขังในที่อยู่อาศัยตลอด 24 ชั่วโมง เว้นแต่กรณีมีนัดหมายทางการแพทย์ นัดมาศาลหรือมีกิจกรรมใด ๆ ซึ่งศาลกำหนดไว้เป็นการเฉพาะ

โดยคดีส่วนใหญ่ในประเทศสหรัฐอเมริกาที่นำมาตรการกักขังที่บ้านมาใช้ เจ้าพนักงานคุมประพฤติหรือพนักงานสืบเสาะจะนำเครื่องมืออิเล็กทรอนิกส์มาใช้ในการควบคุมสอดส่องผู้ถูกควบคุม โดยบุคคลดังกล่าวจะต้องสวมเครื่องมือนี้ที่ข้อเท้าหรือข้อมือตลอดเวลา เครื่องมือนี้จะเป็นตัวรับส่งสัญญาณวิทยุไปยังภาครับเพื่อตรวจสอบว่าผู้ถูกควบคุมยังอยู่ในพื้นที่หรือภายในบ้านหรือไม่ ซึ่งผู้ถูกควบคุมจะต้องอยู่ในบริเวณรัศมีรับส่งสัญญาณของอุปกรณ์ดังกล่าวประมาณ 150 ฟุต โดยตัวรับและส่งสัญญาณนี้จะทำงานร่วมกันในการรายงานการเข้าออกบ้านของผู้ถูกควบคุม[42]

ส่วนในประเทศอังกฤษ มาตรการกักขังในที่อยู่อาศัยและควบคุมด้วยเครื่องมืออิเล็กทรอนิกส์ได้ถูกนำมาใช้ตั้งแต่ปี ค.ศ. 1999 โดยศาลในประเทศอังกฤษอาจนำมาตรการนี้มาใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ได้ 2 กรณี[43] คือ

กรณีแรก ในขั้นตอนก่อนการพิจารณาคดี (Pretrial) ตามกฎหมาย the Bail Act 1976 มาตรา 3AA และกฎหมาย the Children and Young Persons Act 1969 มาตรา 23AA บัญญัติให้อำนาจศาลในการใช้มาตรการกักขังที่บ้านและควบคุมด้วยเครื่องอิเล็กทรอนิกส์กับผู้กระทำผิดที่มีอายุระหว่าง 12-17 ปี ซึ่งอยู่ในระหว่างการประกันตัว

---

[41] United States Courts, “Home Confinement,” <http://www.uscourts.gov/fedprob /supervise/home.html>

[42] *Ibid.*

[43] National Probation Service, “Probation Bench Handbook,” <http://www.probation.homeoffice.gov.uk/files/pdf/Probation%20Bench%20Handbook%202nd%20Edition%202007.pdf>, August 2007.

กรณีที่สอง เป็นการใช้มาตรการกักขังที่บ้านและควบคุมด้วยเครื่องอิเล็กทรอนิกส์ในฐานะของข้อกำหนดใน Community Order หรือการรอการลงโทษ (Suspended Sentence) ตามกฎหมาย the Powers of Criminal Courts (Sentencing) Act 2000 มาตรา 36B บัญญัติให้อำนาจศาลในการกำหนดมาตรการควบคุมด้วยเครื่องมืออิเล็กทรอนิกส์กับผู้กระทำผิดเพื่อควบคุมสอดส่องพฤติกรรมของผู้กระทำผิดในการปฏิบัติตามข้อกำหนดอื่น ๆ ของศาล

เป็นที่น่าสังเกตว่ามาตรการดังกล่าวข้างต้นจำเป็นที่จะต้องใช้ควบคู่กับการจำกัดการเข้าถึงหรือใช้งานคอมพิวเตอร์และอินเทอร์เน็ตด้วย มิฉะนั้นแล้วผู้กระทำความผิดจะมีโอกาสในการกระทำความผิดซ้ำได้โดยง่าย เนื่องจากโดยธรรมชาติของอาชญากรรมทางคอมพิวเตอร์ผู้กระทำความผิดสามารถที่จะก่อภัยได้โดยไม่จำเป็นต้องออกจากที่อยู่อาศัยหรือแม้แต่ออกจากห้องนอนของตน อาศัยแต่เพียงเครื่องคอมพิวเตอร์ส่วนบุคคล กับโมเด็มที่ใช้ในการเชื่อมต่อเข้าสู่ระบบอินเทอร์เน็ตก็สามารถเข้าสู่วงจรในการประกอบอาชญากรรมทางคอมพิวเตอร์ได้แล้ว

ตัวอย่างคดีที่ศาลนำมาตรการการกักขังที่บ้านและการควบคุมโดยเครื่องมืออิเล็กทรอนิกส์มาใช้กับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ เช่น

คดีแฮกเกอร์กลุ่มหนึ่งร่วมกันเจาะระบบคอมพิวเตอร์ขององค์การนาซ่า (NASA) ที่ตั้งอยู่ในเมือง Pasadena มลรัฐแคลิฟอร์เนีย ประเทศสหรัฐอเมริกา ศาลในคดีนี้ตัดสินจำคุกผู้กระทำผิดซึ่งเป็นหัวหน้าของกลุ่มเป็นเวลา 4 เดือนและให้กักขังผู้กระทำผิดในบ้านโดยห้ามใช้งานคอมพิวเตอร์และอินเทอร์เน็ตเป็นเวลา 4 เดือน และนอกจากนี้ผู้กระทำความผิดจะต้องชดใช้เงินค่าเสียหายให้แก่องค์การนาซ่าเป็นเงิน 4,400 เหรียญสหรัฐ[44]

คดี Jerome T. Heckenkamp (U.S. v. Heckenkamp[45] (N.D. Cal.) 25 เมษายน 2005) กระทำความผิดในข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจและทำลายระบบคอมพิวเตอร์ ศาลตัดสินให้จำคุกเป็นเวลา 8 เดือน ปรับเป็นเงิน 268,291 เหรียญสหรัฐ และกักขัง

---

[44] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2 ,p.204.

[45] United States v. Heckenkamp, 482 F.3d 1142 (9th Cir.2007), see also Former Computer Science Graduate Student Sentenced for Hacking Major Corporations: Defendant Jerome Heckenkamp Defaced Web Pages and Installed "Sniffer" Programs to Steal Passwords , < http://www.usdoj.gov/criminal/ cybercrime /heckenkampSent.htm >, 25 April 2005.

ในที่อยู่อาศัยโดยควบคุมด้วยเครื่องอิเล็กทรอนิกส์เป็นระยะเวลา 8 เดือนโดยห้ามจำเลยใช้งานคอมพิวเตอร์เพื่อเข้าถึงระบบอินเทอร์เน็ตโดยไม่ได้รับความยินยอมจากพนักงานคุมประพฤติ

3.1.8 การทำงานบริการสังคม (Community Service)

การทำงานบริการสังคมเป็นเงื่อนไขพิเศษที่ศาลสั่งให้ผู้กระทำความผิดทำงานเพื่อเป็นการชดเชยให้กับชุมชน โดยไม่มีค่าตอบแทนภายใต้การสอดส่องดูแลของพนักงานคุมประพฤติ ทั้งนี้โดยมีวัตถุประสงค์มุ่งไปในแนวทางในการแก้ไขฟื้นฟูผู้กระทำความผิดเป็นหลัก เพราะจะส่งผลให้ผู้กระทำความผิดเกิดความรับผิดชอบทั้งต่อตัวเองและสังคมส่วนรวม สำนึกในความผิดที่ตนได้กระทำไป สำหรับกรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ศาลในต่างประเทศได้นำเอาการทำงานบริการสังคมมาใช้เป็นมาตรการหนึ่งในการแก้ไขฟื้นฟูผู้กระทำผิด

ในประเทศสหรัฐอเมริกา มาตรการทำงานบริการสังคมเป็นเงื่อนไขเพื่อคุมความประพฤติผู้กระทำผิดประการหนึ่งซึ่งศาลสามารถใช้ดุลพินิจในการกำหนดได้และมีบัญญัติไว้ใน Title 18, United State Code (U.S.C.), มาตรา 3563 (b)(12) และนอกจากนี้กฎหมายในแต่ละมลรัฐยังกำหนดให้ศาลอาจนำมาตรการทำงานบริการสังคมมาใช้ในรูปแบบอื่น ๆ ได้ เช่น เป็นเงื่อนไขในการรอลงอาญา (suspended sentence) การปล่อยตัว (discharge) หรือเป็นเงื่อนไขที่ต้องกระทำก่อนการใช้โทษจำคุก (an obligation to be fullfilled before the imprison of formal sentence)[46]

ในประเทศอังกฤษ การทำงานบริการสังคมเป็นข้อกำหนด (Requirement) ใน Community Order ซึ่งมีบัญญัติในกฎหมาย Criminal Justice Act 2003 มาตรา 177 (1)(a) โดยกำหนดให้ศาลอาจมีคำสั่งให้ผู้กระทำผิดซึ่งมีอายุตั้งแต่ 16 ปีขึ้นไปทำงานโดยไม่ได้รับค่าตอบแทน (an unpaid work) ซึ่งศาลจะต้องกำหนดรูปแบบของงานให้เหมาะสมกับผู้กระทำผิด ทั้งนี้โดยมี

---

[46] อนุลักษณ์ สาริกบุตร, “การให้ผู้ถูกคุมความประพฤติทำงานบริการสังคมในฐานะเงื่อนไขของการคุมความประพฤติ: ศึกษาเฉพาะกรณีสำนักงานคุมประพฤติในเขตกรุงเทพมหานคร,” (วิทยานิพนธ์มหาบัณฑิต คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2537), น. 51.

กำหนดระยะเวลาตามระดับความร้ายแรงแห่งคดี อาจแบ่งได้เป็น 3 ระดับ คือ ระดับต่ำ 40-80 ชั่วโมง ระดับกลาง 80-150 ชั่วโมง และระดับสูง 150-300 ชั่วโมง[47]

ตัวอย่างคดีที่ศาลในต่างประเทศนำเอาการทำงานบริการสังคมมาเป็นมาตรการในการแก้ไขฟื้นฟูผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ เช่น คดี Robert Tappan Morris (United States v. Morris[48]) กระทำความผิดตาม 18 U.S.C. มาตรา 1030 (a)(5)(A) ศาลในคดีนี้มีคำสั่งให้จำเลยทำงานบริการสังคมเป็นระยะเวลา 400 ชั่วโมง

3.1.9 โทษกรณีพิเศษ (Special Sanction)

นอกเหนือจากมาตรการบังคับทางอาญาดังที่ได้กล่าวไว้ข้างต้นแล้ว ยังมีมาตรการในรูปแบบอื่นที่ศาลในต่างประเทศนำมาใช้บังคับเป็นกรณีพิเศษ ทั้งนี้อาจจะพิจารณาถึงความเหมาะสมแห่งคดีซึ่งมีลักษณะที่พิเศษเฉพาะเรื่อง ยกตัวอย่างเช่น ในคดีที่เกิดขึ้นในปี ค.ศ.1999 ผู้กระทำผิดซึ่งเป็นเยาวชน อายุเพียง 16 ปี ได้เจาะระบบคอมพิวเตอร์ทางทหารของประเทศสหรัฐอเมริกา (Department of Defense) รวมทั้งระบบคอมพิวเตอร์ขององค์การนาซ่า หรือองค์การอวกาศแห่งชาติสหรัฐอเมริกา (NASA) และได้ขโมยข้อมูลที่สำคัญไป ซึ่งรวมไปถึงโปรแกรมคอมพิวเตอร์ที่มีมูลค่าถึง 1.7 ล้านเหรียญสหรัฐ[49] นอกจากนี้ยังส่งผลให้ระบบคอมพิวเตอร์ของหน่วยงานดังกล่าวใช้การไม่ได้เป็นระยะเวลา 21 วัน ต้องสูญเสียเงินในการซ่อมแซมระบบคอมพิวเตอร์เป็นเงิน 41,000 เหรียญสหรัฐ คดีนี้เป็นคดีที่เกิดจากฝีมือของผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เป็นเยาวชนคดีแรกของประเทศสหรัฐอเมริกา ด้วยเหตุนี้ศาลจึงกำหนดโทษ

---

[47] National Probation Service, “Probation Bench Handbook,” <http://www.probation.homeoffice.gov.uk/files/pdf/Probation%20Bench%20Handbook%202nd%20Edition%202007.pdf>, August 2007.

[48] United States v. Morris, Case Number: 89-CR-139 (Unpublished), Northern District of New York, United States District Court, (May 4, 1990) available at <http://www.rbs2.com/morris.htm>; see also United States v. Morris, 928 F. 2d 504 (2nd Cir.1991).

[49] “เสียงจากแฮกเกอร์,” <http://www.thaiparents.net/articles/title.php?t=72>, เมษายน 2545.

ให้กักกันตัวผู้กระทำผิดไว้ในศูนย์ควบคุมเป็นเวลา 6 เดือน และนอกจากนี้ศาลยังมีคำสั่งให้ผู้กระทำผิดเขียนจดหมายแสดงความเสียใจหรือจดหมายขอโทษไปยังหน่วยงานที่ได้รับความเสียหายจากการกระทำความผิดของตนและผู้กระทำความผิดจะต้อง ยินยอมให้มีการเปิดเผยข้อมูลเกี่ยวกับคดีนี้ให้สาธารณชนได้รับทราบแม้ว่าจะเป็นการฝ่าฝืนกฎหมายว่าด้วยการคุ้มครองข้อมูลของผู้กระทำความผิดที่เป็นเด็กและเยาวชน[50]

3.2 การใช้มาตรการทางอาญาสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ

คดีเกี่ยวกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ ศาลในต่างประเทศมีแนวโน้มในการใช้มาตรการบังคับทางอาญาที่เข้มงวดและรุนแรงมากยิ่งขึ้น ทั้งนี้อาจจะมีสาเหตุ มาจากแนวโน้มของอาชญากรรมทางคอมพิวเตอร์ที่เพิ่มสูงขึ้นและความเสียหายที่เกิดจากการกระทำความผิดทวีความรุนแรงมากยิ่งขึ้น ทำให้ศาลในต่างประเทศเล็งเห็นถึงการนำเอามาตรการบังคับทางอาญามาใช้เป็นเครื่องมือในการควบคุมสังคม ทั้งในแง่ของการข่มขู่ยับยั้งการกระทำความผิด และในแง่การแก้ไขฟื้นฟูผู้กระทำความผิด รวมถึงนำเอามาตรการดังกล่าวมาใช้ในการป้องกันความปลอดภัยของสังคมโดยรวมด้วย

การนำเอามาตรการบังคับทางอาญารูปแบบต่าง ๆ มาใช้สำหรับการกระทำความผิดของอาชญากรคอมพิวเตอร์ในต่างประเทศ ในเบื้องต้นหน่วยงานด้านคุมประพฤติจะเป็นหน่วยงานที่เข้ามามีส่วนสำคัญในการกำหนดมาตรการบังคับต่าง ๆ ที่เหมาะสมแก่ผู้กระทำผิด ซึ่งขั้นตอนนี้เรียกว่า “งานสืบเสาะและพินิจ” (Presentence Investigation) พนักงานคุมประพฤติจะทำหน้าที่ในแสวงหา รวบรวมพยานหลักฐานและวิเคราะห์ข้อเท็จจริงเกี่ยวกับประวัติและภูมิหลังทางสังคมของจำเลยก่อนที่ศาลจะพิพากษาคดี โดยพนักงานคุมประพฤติจะเป็นผู้ดำเนินการตามคำสั่งศาลแล้วรายงาน พร้อมความเห็นและข้อเสนอแนะเพื่อศาลใช้ประกอบดุลพินิจในการพิจารณาพิพากษารอการกำหนดโทษ หรือรอการลงโทษและเลือกใช้วิธีการปฏิบัติที่เหมาะสมกับจำเลยเป็นรายบุคคล[51] Brian J. Kelly[52] พนักงานคุมประพฤติอาวุโส ประเทศสหรัฐอเมริกาและผู้เชี่ยวชาญ

---

[50] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2, p.122.

[51] กรมคุมประพฤติ กระทรวงยุติธรรม, คู่มือตุลาการเกี่ยวกับงานคุมประพฤติ, (กรุงเทพมหานคร : โรงพิมพ์ดอกเบี้ย, 2540), น.3.

พิเศษด้านอาชญากรรมคอมพิวเตอร์ได้กล่าวถึงข้อมูลที่จำเป็น 3 ด้าน ที่พนักงานคุมประพฤติจะต้องสืบเสาะหาข้อเท็จจริงเกี่ยวกับผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์เพื่อนำมาวิเคราะห์หาแนวทางกำหนดโทษเสนอต่อศาล มีดังต่อไปนี้

- ด้านแรก ความรู้และทักษะเกี่ยวกับคอมพิวเตอร์ของผู้กระทำผิด ทั้งนี้รวมถึงประวัติการศึกษา ฝึกอบรมและทำงานในด้านนี้ด้วย
- ด้านที่สอง รายละเอียดเกี่ยวกับคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์อื่น ๆ ซึ่งผู้กระทำผิดเป็นเจ้าของ หรือสามารถเข้าถึงได้
- ด้านที่สาม แรงจูงใจในการกระทำความผิด และวิธีการในการกระทำความผิด ยกตัวอย่างเช่น แรงจูงใจทางการเงินโดยตรง (purely financial) ในกรณีเจาะระบบเข้าไปในเว็บไซต์ซึ่งให้บริการธุรกรรมทางอิเล็กทรอนิกส์เพื่อจารกรรมข้อมูลสำคัญของลูกค้า หรือมีแรงจูงใจอันเนื่องจากความโกรธแค้น ในกรณีที่ลูกจ้างโจมตีระบบคอมพิวเตอร์ของนายจ้าง หรือมีแรงจูงใจต้องการกรรโชกเอาทรัพย์สินจากเหยื่อ (extortion) ตัวอย่างเช่น เจาะระบบเข้าไปในเว็บไซต์ซึ่งให้บริการธุรกรรมทางอิเล็กทรอนิกส์แล้วขโมยข้อมูลสำคัญไปเพื่อข่มขู่เอาทรัพย์สินจากเหยื่อเพื่อแลกกับข้อมูลดังกล่าว

ในขั้นตอนของงานสืบเสาะและพินิจนี้ พนักงานคุมประพฤติจำเป็นต้องสอบถามข้อมูลจากจำเลยเพื่อให้ได้มาซึ่งข้อมูลที่จำเป็นดังกล่าวข้างต้น ตัวอย่างคำถามที่จำเป็นสำหรับการสืบเสาะและพินิจในคดีผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ [53] เช่น

- คุณใช้คอมพิวเตอร์เพื่องานในลักษณะใดบ้าง ?
- คุณเคยเรียนหรือได้รับการฝึกอบรมหรือทำงานด้านคอมพิวเตอร์มาก่อนหรือไม่ ? อย่างไรบ้าง ?

---

[52] Brian J. Kelly, “Supervising the Cyber Criminal,” Federal Probation 65, 2(September 2001): pp.8-10; available at <http://www.uscourts.gov/fedprob/2001 septfp.pdf>.

[53] Mark Sherman, “Special Needs Offenders : Introduction to Cyber Crime,” <http://www.fjc.gov/public/pdf.nsf/lookup/snobull5.pdf/$file/snobull5.pdf>,p.11, August 2000; see also Brian J. Kelly, *supra note* , p.9.

- มีสมาชิกในครอบครัวคนอื่นหรือเพื่อนของคุณที่อาศัยอยู่บริเวณใกล้เคียงและมีคอมพิวเตอร์ด้วยหรือไม่ ?
- คุณเข้าไปใช้บริการของห้องสมุด (ไม่ว่าจะเป็นของสาธารณะหรือเอกชน) ซึ่งจัดให้บริการทางอินเทอร์เน็ตด้วยหรือไม่ ?
- มีบุคคลอื่นอีกหรือไม่ที่เข้าถึงหรือใช้คอมพิวเตอร์ของคุณ ?
- คุณมีคอมพิวเตอร์ที่บ้านทั้งหมดกี่เครื่อง และเป็นคอมพิวเตอร์รูปแบบใด ?

เมื่อพนักงานคุมประพฤติสืบเสาะข้อมูลเกี่ยวกับจำเลยเสร็จเรียบร้อยแล้ว ขั้นตอนต่อมาพนักงานคุมประพฤติจะทำรายงานเสนอความเห็นต่อศาลเกี่ยวกับข้อเท็จจริงเกี่ยวกับตัวจำเลย เช่น อายุ ประวัติ ความประพฤติ สติปัญญา การศึกษาอบรม ฯลฯ และแนวทางในการกำหนดรูปแบบของแนวทางแก้ไขที่เหมาะสมกับจำเลย สำหรับคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในต่างประเทศนั้น ในทางปฏิบัติได้มีการเสนอแนะแนวทางในการกำหนดเงื่อนไขของการคุมประพฤติในส่วนที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ไว้ ดังต่อไปนี้[54]

ตารางที่ 3.1

ข้อเสนอแนะเกี่ยวกับเงื่อนไขเพื่อคุมความประพฤติในส่วนที่เกี่ยวข้องกับการใช้คอมพิวเตอร์[55]

เงื่อนไขเพื่อคุมความประพฤติ	กรณีอนุญาตให้เข้าถึงอินเทอร์เน็ต	กรณีจำกัด/ห้ามเข้าถึงอินเทอร์เน็ต
1. ผู้ถูกคุมความประพฤติจะต้องยินยอมให้พนักงานคุมประพฤติและ/หรือตัวแทนของหน่วยงานคุมประพฤติตรวจสอบอุปกรณ์คอมพิวเตอร์โดยมิจำต้องบอกกล่าวล่วงหน้าได้เป็นระยะ ๆ ทั้งนี้รวมถึงการกู้และคัดลอกหน่วยความจำทั้งหมดจากอุปกรณ์ (hardware) / โปรแกรม (software) และ/หรือการนำเอาอุปกรณ์เช่นว่านั้นไปเพื่อการตรวจสอบ	✓	✓

[54] โปรดดู ตัวอย่างข้อตกลงในการจำกัดและควบคุมสอดส่องการใช้คอมพิวเตอร์ในระหว่างการคุมประพฤติในต่างประเทศ ในภาคผนวก ข.

[55] Arthur L. Bowker and Gregory B. Thompson, “Computer Crime in the 21st Century and Its Effect on the Probation Officer,” Federal Probation (September 2001): p.21. (available at : http://www.uscourts.gov/fedprob/2001septfp.pdf)

และต้องยินยอมให้พนักงานคุมประพฤติติดตั้งอุปกรณ์หรือโปรแกรมใด ๆ ในคอมพิวเตอร์เพื่อตรวจตรา (monitor) การใช้งานคอมพิวเตอร์หรือป้องกันการเข้าถึงข้อมูลต้องห้าม		
2. ห้ามผู้ถูกคุมความประพฤติครอบครองโปรแกรมการเข้ารหัสข้อมูล (encryption) หรือโปรแกรมวิทยาการอำพรางข้อมูล (steganography[56])	✓	✓
3. ผู้ถูกคุมความประพฤติจะต้องให้ข้อมูลที่ถูกต้องแก่พนักงานคุมประพฤติเกี่ยวกับระบบคอมพิวเตอร์และโปรแกรมของผู้ถูกคุมความประพฤติทั้งหมด รวมทั้งรหัสผ่านและผู้จัดให้บริการอินเทอร์เน็ต (ISP: Internet Service Provider) ทั้งหมด	✓	✓
4. ผู้ถูกคุมความประพฤติสามารถครอบครองได้แต่เฉพาะอุปกรณ์คอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ที่ได้รับความเห็นชอบจากพนักงานคุมประพฤติเท่านั้น ทั้งนี้จะต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากพนักงานคุมประพฤติก่อนที่จะได้มาซึ่งอุปกรณ์คอมพิวเตอร์โปรแกรมคอมพิวเตอร์และผู้จัดให้บริการอินเทอร์เน็ต	✓	✓
5. ผู้ถูกคุมความประพฤติจะต้องงดเว้นจากการใช้	✓	✓

[56] วิทยาการอำพรางข้อมูล (steganography) หมายถึง ศาสตร์ในการซ่อนข้อมูลในรูปแบบต่าง ๆ โดยมีจุดมุ่งหมายหลักในการปกปิด ทำให้ดูเหมือนว่าไม่มีการซ่อนข้อมูลลับใด ๆ ในสื่อเป้าหมาย หากมองโดยผิวเผินแล้ว วิทยาการอำพรางข้อมูลมีลักษณะใกล้เคียงกับวิทยาการเข้ารหัสลับ (cryptography) แต่ความแตกต่างของศาสตร์ทั้งสอง คือ การเข้ารหัสมีจุดประสงค์ในการทำให้ข้อความไม่สามารถเข้าใจได้ แต่การอำพรางข้อมูลมีจุดประสงค์ในการซ่อนข้อมูลทำให้คนทั่วไปไม่รู้ว่ามีการซ่อนข้อมูลลับอยู่ ปัจจุบันนี้มีโปรแกรมคอมพิวเตอร์ที่สามารถอำพรางข้อมูลหลายโปรแกรมที่ออกแบบมาเพื่อทำหน้าที่ซ่อนข้อมูลในสื่อดิจิตอล เช่น “S-Tools” หรือ “White Noise Storm” ที่สามารถซ่อนข้อมูลในสื่อที่เป็นรูปภาพ วิดีโอ หรือเพลงได้; ข้อมูลจาก วิกิพีเดียสารานุกรมเสรี < http://th.wikipedia.org >. (ปรับปรุงเนื้อหาล่าสุดเมื่อ 7 กันยายน 2550)

คอมพิวเตอร์ในลักษณะใด ๆ อันอาจจะทำให้ผู้ถูกคุมความประพฤติเข้าไปเกี่ยวข้องกับการกระทำความผิดหรือฝ่าฝืนข้อบังคับ/ เงื่อนไข กล่าวคือ 5.1 _____ 5.2 _____ 5.3 _____		
6. ผู้ถูกคุมความประพฤติจะต้องให้ข้อมูลที่แท้จริงเกี่ยวกับการแสดงตัวตน (Identity) ในอินเทอร์เน็ตหรือการติดต่อสื่อสารทางจดหมายอิเล็กทรอนิกส์ (E-mail) และห้ามเข้าไปในห้องสนทนา (chat room) หรือเว็บไซต์ซึ่ง.....(ขึ้นอยู่กับลักษณะความผิด)	✓	
7. ผู้ถูกคุมความประพฤติจะต้องเก็บบันทึกข้อมูลประจำวันของที่อยู่เว็บไซต์ทั้งหมดที่ผู้ถูกคุมความประพฤติเข้าถึงโดยผ่านทางคอมพิวเตอร์ส่วนบุคคลใด ๆ (หรือคอมพิวเตอร์ของผู้อื่นซึ่งผู้ถูกคุมประพฤติใช้) หรือคอมพิวเตอร์ซึ่งใช้ในการทำงาน และแสดงบันทึกข้อมูลดังกล่าวต่อพนักงานคุมประพฤติ	✓	
8. ห้ามผู้ถูกคุมความประพฤติสร้างหรือให้การสนับสนุนไม่ว่าโดยตรงหรือโดยอ้อมในการสร้างกระดานข่าว (electronic bullentin board) ใด ๆ ผู้จัดให้บริการอินเทอร์เน็ต หรือเครือข่ายคอมพิวเตอร์สาธารณะหรือส่วนบุคคลอื่นใด โดยปราศจากความเห็นชอบเป็นลายลักษณ์อักษรจากพนักงานคุมประพฤติก่อน อนึ่งความเห็นชอบใด ๆ จะต้องอยู่ภายใต้เงื่อนไขซึ่งตั้งโดยสำนักงานคุมประพฤติหรือศาล	✓	✓
9. ห้ามผู้ถูกคุมความประพฤติครอบครองหรือใช้คอมพิวเตอร์ที่เข้าถึงบริการคอมพิวเตอร์ในลักษณะออนไลน์ (รวมถึงในการทำงานหรือการศึกษาด้วย) โดย		✓

ปราศจากความเห็นชอบเป็นลายลักษณ์อักษรจากสำนักงานคุมประพฤติหรือศาลก่อน ทั้งนี้ให้รวมถึงผู้จัดให้บริการอินเทอร์เน็ตใด ๆ ระบบกระดานข่าวหรือเครือข่ายคอมพิวเตอร์สาธารณะหรือส่วนบุคคลใด ๆ อนึ่งความเห็นชอบใด ๆ จะต้องอยู่ภายใต้เงื่อนไขซึ่งตั้งโดยสำนักงานคุมประพฤติหรือศาล		
10. ห้ามผู้ถูกคุมความประพฤติ ซื้อ ครอบครอง หรือได้รับมาซึ่งคอมพิวเตอร์ส่วนบุคคลซึ่งติดตั้งโมเด็มภายในเครื่องและ/หรือโมเด็มภายนอก (external modem)		✓
11. ในกรณีที่ผู้ถูกคุมความประพฤติทำงานเป็นผู้ติดตั้งอุปกรณ์คอมพิวเตอร์ โปรแกรมเมอร์ หรือผู้เชี่ยวชาญในด้านแก้ปัญหา (trouble shooter) เกี่ยวกับคอมพิวเตอร์ ผู้ถูกคุมความประพฤติจะต้องอยู่ภายใต้เงื่อนไขเกี่ยวกับการประกอบอาชีพในระหว่างการคุมประพฤติ กล่าวคือ ผู้ถูกคุมประพฤติไม่สามารถทำงานดังกล่าวได้ไม่ว่าโดยตรงหรือโดยอ้อม	✓	✓

ประเด็นในเรื่องความเหมาะสมของมาตรการบังคับทางอาญาสำหรับคดีเกี่ยวกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบได้กลายเป็นประเด็นข้อถกเถียงในเวลาต่อมาว่า ในบางคดีศาลเข้มงวดกับเงื่อนไขในการควบคุมความประพฤติของผู้ต้องโทษมากเกินไปหรือไม่ ยกตัวอย่างเช่นในคดีชื่อดัง อย่างนายเควิน มิตนิก ซึ่งในคดีนี้ศาลได้กำหนดรายละเอียดในการควบคุมพฤติกรรมของผู้กระทำผิดไว้อย่างเข้มงวด แม้ว่าศาลจะอ้างเหตุผลในการมีคำสั่งเช่นนั้นว่าเป็นการคุ้มครองความปลอดภัยของสังคมจากการก่อภัยจากตัวผู้ต้องโทษซึ่งเป็นผู้กระทำผิดที่กระทำความผิดติดนิสัย แต่อย่างไรก็ตามยังมีข้อถกเถียงว่าคำสั่งดังกล่าวเป็นการก้าวล่วงสิทธิของจำเลยมากเกินควรหรือไม่[57]

[57] United States v. Mitnick, 145 F. 3d 1342 (9th Cir. 1998); see also Christopher M.E. Painter, “Supervised Release and Probation Restrictions in Hacker

จากการศึกษาของ Smith และคณะ[58] พบว่า ในคดีเกี่ยวกับอาชญากรคอมพิวเตอร์ศาลในต่างประเทศมีแนวทางในการพิจารณาถึงปัจจัยความร้ายแรงแห่งคดีจากหลาย ๆ ปัจจัย ยกตัวอย่างเช่น ความเสียหายจากการกระทำความผิด (Financial Loss) การกระทำความผิดต่อหน่วยงานของราชการ (Breaching Government Agency's Systems) การกระทำความผิดในอำนาจหน้าที่ (Breach of Trust) ทักษะความสามารถของผู้กระทำผิด (Special Skill) รวมถึงความเชี่ยวชาญและความซับซ้อนในการวางแผน (Sophishtication Planning and Expertise) เป็นต้น ปัจจัยต่าง ๆ เหล่านี้ศาลในต่างประเทศจะนำมาใช้ในการพิจารณาถึงความร้ายแรงแห่งคดีอันจะส่งผลให้ผู้กระทำความผิดได้รับโทษที่รุนแรงยิ่งขึ้น ในทางตรงกันข้าม มีปัจจัยบางประการที่ศาลหยิบยกหรือคู่ความกล่าวอ้างเพื่อเป็นประโยชน์ในการลดหย่อนผ่อนโทษ เช่น การปราศจากเจตนามุ่งร้ายต่อเหยื่อ (Lack of malicious intent) หรือปัญหาอาการในด้านสุขภาพจิตของผู้กระทำผิดเกี่ยวกับอาการเสพติดอินเทอร์เน็ตหรือการเจาะระบบ (Mental health problems including computer/Internet addiction) เป็นต้น แต่อย่างไรก็ตามปัจจัยต่าง ๆ เหล่านี้เป็นแต่เพียงข้อพิจารณาประการหนึ่งของศาลที่จะนำมาใช้ในการประกอบการกำหนดโทษในคดีเท่านั้น ทั้งนี้จึงขึ้นอยู่กับดุลพินิจของศาลในแต่ละคดีว่าจะกำหนดโทษให้หนักหรือเบามากน้อยเพียงใด

นอกจากนี้ Smith และคณะยังได้รวบรวมข้อมูลเชิงสถิติเกี่ยวกับการลงโทษในคดีเกี่ยวกับการกระทำความผิดของอาชญากรคอมพิวเตอร์ในแต่ละประเทศ แต่ละภูมิภาค ซึ่งผู้ศึกษาเห็นว่าเป็นประโยชน์ในการทำความเข้าใจภาพรวมของการใช้มาตรการบังคับทางอาญาสำหรับการกระทำความผิดของอาชญากรคอมพิวเตอร์ในแต่ละประเทศ แต่ละภูมิภาคว่ามีแนวโน้มในการนำมาใช้กับคดีลักษณะนี้มากน้อยเพียงใด แต่อย่างไรก็ดีข้อมูลดังกล่าวเป็นแต่เพียงการรวบรวมจากคำพิพากษาส่วนหนึ่งเท่านั้นและไม่อาจชี้วัดถึงความเหมาะสมของมาตรการบังคับทางอาญาในแต่ละรูปแบบได้ รายละเอียดมีดังต่อไปนี้

Cases," <http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm>; see also United States v. Lifshitz, 369 F.3d 173, 193 (2d Cir. 2004).

[58] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2, pp.106-150.